Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft’s May 2026 Patch Tuesday

Date of Publication	Admiralty Code	TA Number
May 13, 2026	A1	TA2026129

Summary

First Seen: May 12, 2026
Affected Platforms: Microsoft SQL Server, Windows Kernel, Windows Hyper-V, Microsoft Office, Microsoft SharePoint, Google Chromium and more
Impact: Information Disclosure, Denial of Service, Remote Code Execution, Elevation of Privilege, Security Feature Bypass, Spoofing, Tampering

Exploitable CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-33835	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	✗	✗	✓
CVE-2026-33837	Windows TCP/IP Local Elevation of Privilege Vulnerability	Windows TCP/IP	✗	✗	✓
CVE-2026-33840	Win32k Elevation of Privilege Vulnerability	Windows Win32K - ICOMP	✗	✗	✓
CVE-2026-33841	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	✗	✗	✓
CVE-2026-35416	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	✗	✗	✓
CVE-2026-35417	Windows Win32k Elevation of Privilege Vulnerability	Windows Win32K - ICOMP	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-35435	Azure AI Foundry Elevation of Privilege Vulnerability	Azure AI Foundry M365 published agents	✗	✗	✓
CVE-2026-40361	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	✗	✗	✓
CVE-2026-40364	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	✗	✗	✓
CVE-2026-40369	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	✗	✗	✓
CVE-2026-40397	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	✗	✗	✓
CVE-2026-40398	Windows Remote Desktop Services Elevation of Privilege Vulnerability	Windows Remote Desktop	✗	✗	✓
CVE-2026-41103	Microsoft SSO Plugin for Jira & Confluence Elevation of Privilege Vulnerability	Microsoft SSO Plugin for Jira & Confluence	✗	✗	✓
CVE-2026-35420	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	✗	✗	✓
CVE-2026-41089	Windows Netlogon Remote Code Execution Vulnerability	Windows Netlogon	✗	✗	✓
CVE-2026-40402	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Hyper-V	✗	✗	✓

Note: The exploitable CVEs have patch links hyperlinked to the corresponding tick marks.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1189: Drive-by Compromise	
	T1566: Phishing	T1566.001: Spearphishing Attachment
		T1566.002: Spearphishing Link
Execution	T1203: Exploitation for Client Execution	
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1204: User Execution	T1204.001: Malicious Link
		T1204.002: Malicious File
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1553: Subvert Trust Controls	T1553.006: Code Signing Policy Modification
Privilege Escalation	T1611: Escape to Host	
	T1068: Exploitation for Privilege Escalation	
	T1542: Pre-OS Boot	T1542.003: Bootkit
Credential Access	T1552: Unsecured Credentials	
	T1556: Modify Authentication Process	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
	T1210: Exploitation of Remote Services	
Impact	T1499: Endpoint Denial of Service	

Vulnerability Details

#1

Microsoft's May 2026 Patch Tuesday delivers a significant security update, addressing 137 vulnerabilities across its product ecosystem. Of these, 30 are rated Critical, 103 Important, and 4 Moderate. The vulnerabilities span multiple impact categories, including 62 Elevation of Privilege (EoP), 31 Remote Code Execution (RCE), 15 Information Disclosure, 13 Spoofing, 8 Denial of Service (DoS), 6 Security Feature Bypass, and 2 Tampering flaws.

#2

Elevation of Privilege vulnerabilities alone account for over 50% of this month's patches, reflecting a continued attacker focus on post-compromise privilege escalation. Microsoft also resolved 128 non-Microsoft vulnerabilities, including Chromium-based Edge flaws, bringing the total to 265. Notably, 16 CVEs are assessed as at increased risk of exploitation, underscoring the urgency of deploying patches promptly. Notably, this is the first zero-day-free Patch Tuesday since June 2024, breaking a 22-month streak.

#3

The most critical infrastructure vulnerability is CVE-2026-41089, a stack-based buffer overflow in Windows Netlogon (CVSS 9.8) that allows an unauthenticated attacker to execute code on a domain controller by sending a specially crafted network request. No privileges or user interaction are required, and attack complexity is low, a compromised domain controller effectively means a compromised domain, making this the top remediation priority.

#4

CVE-2026-41103, an Elevation of Privilege vulnerability in the Microsoft SSO Plugin for Jira & Confluence (CVSS 9.1), allows an unauthenticated attacker to send a specially crafted SSO response during login and trick the system into accepting a forged identity, bypassing Microsoft Entra ID authentication entirely. This is particularly dangerous for organizations with Atlassian-integrated environments.

#5

CVE-2026-40402, a use-after-free in Windows Hyper-V (CVSS 9.3), enables a guest-to-host escape allowing an attacker to gain SYSTEM privileges on the Hyper-V host, making it critical for multi-tenant and private cloud environments where a single boundary failure can compromise multiple workloads.

#6

Two Critical RCEs in Microsoft Word, CVE-2026-40361 and CVE-2026-40364, can be triggered via the Preview Pane without opening the malicious document, continuing a dangerous document-driven attack pattern from previous months. This makes Office endpoint patching an urgent priority, particularly in environments where employees regularly receive external attachments.

#7

CVE-2026-35435, an Elevation of Privilege vulnerability in Azure AI Foundry M365 published agents, stems from improper access control and could allow an unauthenticated attacker to elevate privileges over a network, highlighting the expanding AI-connected enterprise attack surface. Microsoft has noted that no customer action is required as this was mitigated server-side.

#8

The Elevation of Privilege vulnerabilities dominating this release target deeply trusted Windows components. CVE-2026-33841 and CVE-2026-40369 affect the Windows Kernel and could allow a local attacker to elevate to SYSTEM level, bringing the total Windows Kernel EoP vulnerabilities patched in 2026 to 13. CVE-2026-33837, a heap-based buffer overflow in Windows TCP/IP (tcpip.sys), enables local privilege escalation.

#9

Additional EoP flaws targeting critical kernel-adjacent components include CVE-2026-33835 (Windows Cloud Files Mini Filter Driver), CVE-2026-33840 (Win32k - ICOMP), CVE-2026-35416 (Windows Ancillary Function Driver for WinSock), CVE-2026-35417 (Windows Win32k), CVE-2026-35420 (Windows Kernel), CVE-2026-40397 (Windows Common Log File System Driver), and CVE-2026-40398 (Windows Remote Desktop Services), all enabling SYSTEM-level privilege escalation. The CLFS driver in particular has a long history of weaponization in real-world attack chains, making CVE-2026-40397 a priority despite its "Important" rating.

#10

Organizations should prioritize patching domain controllers (Netlogon), Hyper-V hosts, Office endpoints, and systems running the CLFS driver, Win32k, TCP/IP, and WinSock components. Environments using the Microsoft SSO Plugin for Jira & Confluence should treat CVE-2026-41103 as an emergency deployment. With the Secure Boot certificate expiration deadline on June 26, 2026 now just 45 days away, this release represents the final comfortable deployment window before that critical milestone, and organizations should validate Secure Boot certificate status across the fleet without delay.

Recommendations

Conduct an extensive service exposure evaluation to identify any vulnerable services that may be publicly accessible. Take immediate and decisive action to address any identified vulnerabilities, either by installing essential **patches** or adopting security measures.

Keep your systems up to date by implementing the most recent security updates. To avoid the introduction of new vulnerabilities, follow security rules adapted to unique devices. Furthermore, to strengthen the resilience of devices and apps exposed to the internet, thoroughly review their configurations.

Prioritize patching the high-severity vulnerabilities CVE-2026-41103, CVE-2026-41089, CVE-2026-40402, CVE-2026-40361 and CVE-2026-40364. These vulnerabilities pose significant exploitation risks and should be addressed urgently.

Implement network segmentation to restrict unauthorized access and reduce the impact of potential attacks. This can be especially effective in scenarios where network adjacency is a factor.

Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks. This strategy reduces the effects of vulnerabilities related to privilege escalation.

All CVEs

CVE	NAME	PRODUCT	IMPACT
CVE-2026-21530	Windows Rich Text Edit Elevation of Privilege Vulnerability	Windows Rich Text Edit	Elevation of Privilege
CVE-2026-26129	M365 Copilot Information Disclosure Vulnerability	M365 Copilot	Information Disclosure
CVE-2026-26164	M365 Copilot Information Disclosure Vulnerability	M365 Copilot	Information Disclosure
CVE-2026-32161	Windows Native WiFi Miniport Driver Remote Code Execution Vulnerability	Windows Native WiFi Miniport Driver	Remote Code Execution
CVE-2026-32170	Windows Rich Text Edit Elevation of Privilege Vulnerability	Windows Rich Text Edit Control	Elevation of Privilege
CVE-2026-32175	.NET Core Tampering Vulnerability	.NET	Tampering
CVE-2026-32177	.NET Elevation of Privilege Vulnerability	.NET	Elevation of Privilege
CVE-2026-32185	Microsoft Teams Spoofing Vulnerability	Microsoft Teams	Spoofing
CVE-2026-32204	Azure Monitor Agent Elevation of Privilege Vulnerability	Azure Monitor Agent	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-32207	Azure Machine Learning Notebook Spoofing Vulnerability	Azure Machine Learning	Spoofing
CVE-2026-32209	Windows Filtering Platform (WFP) Security Feature Bypass Vulnerability	Windows Filtering Platform (WFP)	Security Feature Bypass
CVE-2026-33109	Azure Managed Instance for Apache Cassandra Remote Code Execution Vulnerability	Azure Managed Instance for Apache Cassandra	Remote Code Execution
CVE-2026-33110	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-33111	Copilot Chat (Microsoft Edge) Information Disclosure Vulnerability	Copilot Chat (Microsoft Edge)	Information Disclosure
CVE-2026-33112	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-33117	Azure SDK for Java Security Feature Bypass Vulnerability	Azure SDK	Security Feature Bypass
CVE-2026-33821	Microsoft Dynamics 365 Customer Insights Elevation of Privilege Vulnerability	Microsoft Dynamics 365 Customer Insights	Elevation of Privilege
CVE-2026-33823	Microsoft Team Events Portal Information Disclosure Vulnerability	Microsoft Teams	Information Disclosure
CVE-2026-33833	Azure Machine Learning Notebook Spoofing Vulnerability	Azure Machine Learning	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2026-33834	Windows Event Logging Service Elevation of Privilege Vulnerability	Windows Event Logging Service	Elevation of Privilege
CVE-2026-33835	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	Elevation of Privilege
CVE-2026-33837	Windows TCP/IP Local Elevation of Privilege Vulnerability	Windows TCP/IP	Elevation of Privilege
CVE-2026-33838	Windows Message Queuing (MSMQ) Elevation of Privilege Vulnerability	Windows Message Queuing	Elevation of Privilege
CVE-2026-33839	Win32k Elevation of Privilege Vulnerability	Windows Win32K - GRFX	Elevation of Privilege
CVE-2026-33840	Win32k Elevation of Privilege Vulnerability	Windows Win32K - ICOMP	Elevation of Privilege
CVE-2026-33841	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-33844	Azure Managed Instance for Apache Cassandra Remote Code Execution Vulnerability	Azure Managed Instance for Apache Cassandra	Remote Code Execution
CVE-2026-34327	Microsoft Partner Center Spoofing Vulnerability	Microsoft Partner Center	Spoofing
CVE-2026-34329	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	Windows Message Queuing	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-34330	Win32k Elevation of Privilege Vulnerability	Windows Win32K - GRFX	Elevation of Privilege
CVE-2026-34331	Win32k Elevation of Privilege Vulnerability	Windows Win32K - GRFX	Elevation of Privilege
CVE-2026-34332	Windows Kernel-Mode Driver Remote Code Execution Vulnerability	Windows Kernel-Mode Drivers	Remote Code Execution
CVE-2026-34333	Windows Win32k Elevation of Privilege Vulnerability	Windows Win32K - GRFX	Elevation of Privilege
CVE-2026-34334	Windows TCP/IP Elevation of Privilege Vulnerability	Windows TCP/IP	Elevation of Privilege
CVE-2026-34336	Windows DWM Core Library Information Disclosure Vulnerability	Windows DWM Core Library	Information Disclosure
CVE-2026-34337	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	Elevation of Privilege
CVE-2026-34338	Windows Telephony Service Elevation of Privilege Vulnerability	Windows Telephony Service	Elevation of Privilege
CVE-2026-34339	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability	Windows LDAP - Lightweight Directory Access Protocol	Denial of Service
CVE-2026-34340	Windows Projected File System Elevation of Privilege Vulnerability	Windows Projected File System	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-34341	Windows Link-Layer Discovery Protocol (LLDP) Elevation of Privilege Vulnerability	Windows Link-Layer Discovery Protocol (LLDP)	Elevation of Privilege
CVE-2026-34342	Windows Print Spooler Elevation of Privilege Vulnerability	Windows Print Spooler Components	Elevation of Privilege
CVE-2026-34343	Windows Application Identity (AppID) Subsystem Elevation of Privilege Vulnerability	Windows Application Identity (AppID) Subsystem	Elevation of Privilege
CVE-2026-34344	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-34345	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-34347	Windows Win32k Elevation of Privilege Vulnerability	Windows Win32K - GRFX	Elevation of Privilege
CVE-2026-34350	Windows Storport Miniport Driver Denial of Service Vulnerability	Windows Storport Miniport Driver	Denial of Service
CVE-2026-34351	Windows TCP/IP Elevation of Privilege Vulnerability	Windows TCP/IP	Elevation of Privilege
CVE-2026-35415	Windows Storage Spaces Controller Elevation of Privilege Vulnerability	Windows Storage Spaces Controller	Elevation of Privilege
CVE-2026-35416	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege

CVE	NAME	PRODUCT	IMPACT
CVE-2026-35417	Windows Win32k Elevation of Privilege Vulnerability	Windows Win32K - ICOMP	Elevation of Privilege
CVE-2026-35418	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	Windows Cloud Files Mini Filter Driver	Elevation of Privilege
CVE-2026-35419	Windows DWM Core Library Information Disclosure Vulnerability	Windows DWM Core Library	Information Disclosure
CVE-2026-35420	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-35421	Windows GDI Remote Code Execution Vulnerability	Windows GDI	Remote Code Execution
CVE-2026-35422	Windows TCP/IP Driver Security Feature Bypass Vulnerability	Windows TCP/IP	Security Feature Bypass
CVE-2026-35423	Windows 11 Telnet Client Information Disclosure Vulnerability	Telnet Client	Information Disclosure
CVE-2026-35424	Internet Key Exchange (IKE) Protocol Denial of Service Vulnerability	Windows Internet Key Exchange (IKE) Protocol	Denial of Service
CVE-2026-35428	Azure Cloud Shell Spoofing Vulnerability	Azure Cloud Shell	Spoofing
CVE-2026-35429	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability	Microsoft Edge for Android	Spoofing

CVE	NAME	PRODUCT	IMPACT
CVE-2026-35433	.NET Elevation of Privilege Vulnerability	.NET	Elevation of Privilege
CVE-2026-35435	Azure AI Foundry Elevation of Privilege Vulnerability	Azure AI Foundry M365 published agents	Elevation of Privilege
CVE-2026-35436	Microsoft Office Click-To-Run Elevation of Privilege Vulnerability	Microsoft Office Click-To-Run	Elevation of Privilege
CVE-2026-35438	Windows Admin Center Elevation of Privilege Vulnerability	Windows Admin Center	Elevation of Privilege
CVE-2026-35439	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-35440	Microsoft Word Information Disclosure Vulnerability	Microsoft Office Word	Information Disclosure
CVE-2026-40357	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-40358	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-40359	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-40360	Microsoft Excel Information Disclosure Vulnerability	Microsoft Office Excel	Information Disclosure

CVE	NAME	PRODUCT	IMPACT
CVE-2026-40361	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-40362	Microsoft Excel Remote Code Execution Vulnerability	Microsoft Office Excel	Remote Code Execution
CVE-2026-40363	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution
CVE-2026-40364	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-40365	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-40366	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-40367	Microsoft Word Remote Code Execution Vulnerability	Microsoft Office Word	Remote Code Execution
CVE-2026-40368	Microsoft SharePoint Server Remote Code Execution Vulnerability	Microsoft Office SharePoint	Remote Code Execution
CVE-2026-40369	Windows Kernel Elevation of Privilege Vulnerability	Windows Kernel	Elevation of Privilege
CVE-2026-40370	SQL Server Remote Code Execution Vulnerability	SQL Server	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-40374	Microsoft Power Automate Desktop Information Disclosure Vulnerability	Power Automate	Information Disclosure
CVE-2026-40377	Microsoft Cryptographic Services Elevation of Privilege Vulnerability	Windows Cryptographic Services	Elevation of Privilege
CVE-2026-40379	Microsoft Enterprise Security Token Service (ESTS) Spoofing Vulnerability	Azure Entra ID	Spoofing
CVE-2026-40380	Windows Volume Manager Extension Driver Remote Code Execution Vulnerability	Windows Volume Manager Extension Driver	Remote Code Execution
CVE-2026-40381	Azure Connected Machine Agent Elevation of Privilege Vulnerability	Azure Connected Machine Agent	Elevation of Privilege
CVE-2026-40382	Windows Telephony Service Elevation of Privilege Vulnerability	Windows Telephony Service	Elevation of Privilege
CVE-2026-40397	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	Elevation of Privilege
CVE-2026-40398	Windows Remote Desktop Services Elevation of Privilege Vulnerability	Windows Remote Desktop	Elevation of Privilege
CVE-2026-40399	Windows TCP/IP Elevation of Privilege Vulnerability	Windows TCP/IP	Elevation of Privilege
CVE-2026-40401	Windows TCP/IP Denial of Service Vulnerability	Windows TCP/IP	Denial of Service

CVE	NAME	PRODUCT	IMPACT
CVE-2026-40402	Windows Hyper-V Elevation of Privilege Vulnerability	Windows Hyper-V	Elevation of Privilege
CVE-2026-40403	Windows Graphics Component Remote Code Execution Vulnerability	Windows Win32K - GRFX	Remote Code Execution
CVE-2026-40405	Windows TCP/IP Denial of Service Vulnerability	Windows TCP/IP	Denial of Service
CVE-2026-40406	Windows TCP/IP Information Disclosure Vulnerability	Windows TCP/IP	Information Disclosure
CVE-2026-40407	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Windows Common Log File System Driver	Elevation of Privilege
CVE-2026-40408	Windows WAN ARP Driver Elevation of Privilege Vulnerability	Windows Kernel-Mode Drivers	Elevation of Privilege
CVE-2026-40410	Windows SMB Client Elevation of Privilege Vulnerability	Windows SMB Client	Elevation of Privilege
CVE-2026-40413	Windows TCP/IP Denial of Service Vulnerability	Windows TCP/IP	Denial of Service
CVE-2026-40414	Windows TCP/IP Denial of Service Vulnerability	Windows TCP/IP	Denial of Service
CVE-2026-40415	Windows TCP/IP Remote Code Execution Vulnerability	Windows TCP/IP	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-40416	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-40417	Microsoft Dynamics 365 Business Central Elevation of Privilege Vulnerability	Dynamics Business Central	Elevation of Privilege
CVE-2026-40418	Microsoft Office Click-To-Run Elevation of Privilege Vulnerability	Microsoft Office Click-To-Run	Elevation of Privilege
CVE-2026-40419	Microsoft Office Click-To-Run Elevation of Privilege Vulnerability	Microsoft Office	Elevation of Privilege
CVE-2026-40420	Microsoft Office Click-To-Run Elevation of Privilege Vulnerability	Microsoft Office Click-To-Run	Elevation of Privilege
CVE-2026-40421	Microsoft Word Information Disclosure Vulnerability	Microsoft Office Word	Information Disclosure
CVE-2026-41086	Windows Admin Center in Azure Portal Elevation of Privilege Vulnerability	Windows Admin Center	Elevation of Privilege
CVE-2026-41088	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	Windows Ancillary Function Driver for WinSock	Elevation of Privilege
CVE-2026-41089	Windows Netlogon Remote Code Execution Vulnerability	Windows Netlogon	Remote Code Execution
CVE-2026-41094	Microsoft Data Formulator Remote Code Execution Vulnerability	Microsoft Data Formulator	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-41095	Data Deduplication Elevation of Privilege Vulnerability	Data Deduplication	Elevation of Privilege
CVE-2026-41096	Windows DNS Client Remote Code Execution Vulnerability	Microsoft Windows DNS	Remote Code Execution
CVE-2026-41097	Secure Boot Security Feature Bypass Vulnerability	Windows Secure Boot	Security Feature Bypass
CVE-2026-41100	Microsoft 365 Copilot for Android Spoofing Vulnerability	M365 Copilot	Spoofing
CVE-2026-41101	Microsoft Word for Android Spoofing Vulnerability	Microsoft Office Word	Spoofing
CVE-2026-41102	Microsoft PowerPoint for Android Spoofing Vulnerability	Microsoft Office PowerPoint	Spoofing
CVE-2026-41103	Microsoft SSO Plugin for Jira & Confluence Elevation of Privilege Vulnerability	Microsoft SSO Plugin for Jira & Confluence	Elevation of Privilege
CVE-2026-41105	Azure Monitor Action Group Notification System Elevation of Privilege Vulnerability	Azure Notification Service	Elevation of Privilege
CVE-2026-41107	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-41109	GitHub Copilot and Visual Studio Code Security Feature Bypass Vulnerability	GitHub Copilot and Visual Studio	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2026-41610	Visual Studio Code Security Feature Bypass Vulnerability	Visual Studio Code	Security Feature Bypass
CVE-2026-41611	Visual Studio Code Remote Code Execution Vulnerability	Visual Studio Code	Remote Code Execution
CVE-2026-41612	Visual Studio Code Information Disclosure Vulnerability	Visual Studio Code	Information Disclosure
CVE-2026-41613	Visual Studio Code Elevation of Privilege Vulnerability	Visual Studio Code	Elevation of Privilege
CVE-2026-41614	M365 Copilot for Desktop Spoofing Vulnerability	M365 Copilot for Desktop	Spoofing
CVE-2026-42823	Azure Logic Apps Elevation of Privilege Vulnerability	Azure Logic Apps	Elevation of Privilege
CVE-2026-42825	Windows Telephony Service Elevation of Privilege Vulnerability	Windows Telephony Service	Elevation of Privilege
CVE-2026-42826	Azure DevOps Information Disclosure Vulnerability	Azure DevOps	Information Disclosure
CVE-2026-42830	Azure Monitor Agent Metrics Extension Elevation of Privilege Vulnerability	Azure Monitor Agent	Elevation of Privilege
CVE-2026-42831	Microsoft Office Remote Code Execution Vulnerability	Microsoft Office	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-42832	Microsoft Office Spoofing Vulnerability	Microsoft Office	Spoofing
CVE-2026-42833	Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability	Microsoft Dynamics 365 (on-premises)	Remote Code Execution
CVE-2026-42838	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Microsoft Edge (Chromium-based)	Elevation of Privilege
CVE-2026-42891	Microsoft Edge (Chromium-based) for Android Spoofing Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-42893	Microsoft Outlook for iOS Tampering Vulnerability	M365 Copilot	Tampering
CVE-2026-42896	Windows DWM Core Library Elevation of Privilege Vulnerability	Windows DWM Core Library	Elevation of Privilege
CVE-2026-42898	Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability	Microsoft Dynamics 365 (on-premises)	Remote Code Execution
CVE-2026-42899	ASP.NET Core Denial of Service Vulnerability	ASP.NET Core	Denial of Service
CVE-2025-54518	AMD: CVE-2025-54518 CPU OP Cache Corruption	AMD CPU Branch	Elevation of Privilege
CVE-2026-7896	Chromium Integer overflow in Blink Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7897	Chromium Use after free in Mobile Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7898	Chromium Use after free in Chromoting Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7899	Chromium Out of bounds read and write in V8 Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7900	Chromium Heap buffer overflow in ANGLE Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7901	Chromium Use after free in ANGLE Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7902	Chromium Out of bounds memory access in V8 Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7903	Chromium Integer overflow in ANGLE Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7904	Chromium Out of bounds read in Fonts Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7905	Chromium Insufficient validation of untrusted input in Media Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7906	Chromium Use after free in SVG Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7907	Chromium Use after free in DOM Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7908	Chromium Use after free in Fullscreen Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7909	Chromium Inappropriate implementation in ServiceWorker Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7910	Chromium Use after free in Views Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7911	Chromium Use after free in Aura Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7912	Chromium Integer overflow in GPU Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7913	Chromium Insufficient policy enforcement in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7914	Chromium Type Confusion in Accessibility Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7915	Chromium Insufficient data validation in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7916	Chromium Insufficient data validation in InterestGroups Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7917	Chromium Use after free in Fullscreen Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7918	Chromium Use after free in GPU Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7919	Chromium Use after free in Aura Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7920	Chromium Use after free in Skia Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7921	Chromium Use after free in Passwords Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7922	Chromium Use after free in ServiceWorker Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7923	Chromium Out of bounds write in Skia Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7924	Chromium Uninitialized Use in Dawn Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7925	Chromium Use after free in Chromoting Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7926	Chromium Use after free in PresentationAPI Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7927	Chromium Type Confusion in Runtime Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7928	Chromium Use after free in WebRTC Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7929	Chromium Use after free in MediaRecording Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7930	Chromium Insufficient validation of untrusted input in Cookies Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7931	Chromium Insufficient validation of untrusted input in iOS Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7932	Chromium Insufficient policy enforcement in Downloads Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7933	Chromium Out of bounds read in WebCodecs Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7934	Chromium Insufficient validation of untrusted input in Popup Blocker Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7935	Chromium Inappropriate implementation in Speech Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7936	Chromium Object lifecycle issue in V8 Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7937	Chromium Insufficient policy enforcement in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7938	Chromium Use after free in CSS Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7939	Chromium Inappropriate implementation in SanitizerAPI Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7940	Chromium Use after free in V8 Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7941	Chromium Insufficient validation of untrusted input in Mobile Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7942	Chromium Integer overflow in ANGLE Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7943	Chromium Insufficient validation of untrusted input in ANGLE Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7944	Chromium Insufficient validation of untrusted input in Persistent Cache Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7945	Chromium Insufficient validation of untrusted input in COOP Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7946	Chromium Insufficient policy enforcement in WebUI Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7947	Chromium Insufficient validation of untrusted input in Network Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7948	Chromium Race in Chromoting Vulnerability	Microsoft Edge (Chromium-based)	Denial of Service
CVE-2026-7949	Chromium Out of bounds read in Skia Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7950	Chromium Out of bounds read and write in GFX Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7951	Chromium Out of bounds write in WebRTC Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7952	Chromium Insufficient policy enforcement in Extensions Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7953	Chromium Insufficient validation of untrusted input in Omnibox Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7954	Chromium Race in Shared Storage Vulnerability	Microsoft Edge (Chromium-based)	Denial of Service
CVE-2026-7955	Chromium Uninitialized Use in GPU Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7956	Chromium Use after free in Navigation Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7957	Chromium Out of bounds write in Media Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7958	Chromium Inappropriate implementation in ServiceWorker Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7959	Chromium Inappropriate implementation in Navigation Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7960	Chromium Race in Speech Vulnerability	Microsoft Edge (Chromium-based)	Denial of Service
CVE-2026-7961	Chromium Insufficient validation of untrusted input in Permissions Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7962	Chromium Insufficient policy enforcement in DirectSockets Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7963	Chromium Inappropriate implementation in ServiceWorker Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7964	Chromium Insufficient validation of untrusted input in FileSystem Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7965	Chromium Insufficient validation of untrusted input in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7966	Chromium Insufficient validation of untrusted input in SiteIsolation Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7967	Chromium Insufficient validation of untrusted input in Navigation Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7968	Chromium Insufficient validation of untrusted input in CORS Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7969	Chromium Integer overflow in Network Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7970	Chromium Use after free in TopChrome Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7971	Chromium Inappropriate implementation in ORB Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7972	Chromium Uninitialized Use in GPU Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7973	Chromium Integer overflow in Dawn Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7974	Chromium Use after free in Blink Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7975	Chromium Use after free in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7976	Chromium Use after free in Views Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7977	Chromium Inappropriate implementation in Canvas Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7978	Chromium Inappropriate implementation in Companion Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7979	Chromium Inappropriate implementation in Media Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7980	Chromium Use after free in WebAudio Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7981	Chromium Out of bounds read in Codecs Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7982	Chromium Uninitialized Use in WebCodecs Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7983	Chromium Out of bounds read in Dawn Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7984	Chromium Use after free in ReadingMode Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7985	Chromium Use after free in GPU Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7986	Chromium Insufficient policy enforcement in Autofill Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7987	Chromium Use after free in WebRTC Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7988	Chromium Type Confusion in WebRTC Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7989	Chromium Insufficient data validation in DataTransfer Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7990	Chromium Insufficient validation of untrusted input in Updater Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7991	Chromium Use after free in UI Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-7992	Chromium Insufficient validation of untrusted input in UI Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7993	Chromium Insufficient validation of untrusted input in Payments Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7994	Chromium Inappropriate implementation in Chromoting Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-7995	Chromium Out of bounds read in AdFilter Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-7996	Chromium Insufficient validation of untrusted input in SSL Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2026-7997	Chromium Insufficient validation of untrusted input in Updater Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7998	Chromium Insufficient validation of untrusted input in Dialog Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-7999	Chromium Inappropriate implementation in V8 Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-8000	Chromium Insufficient validation of untrusted input in ChromeDriver Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8001	Chromium Use after free in Printing Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-8002	Chromium Use after free in Audio Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution
CVE-2026-8003	Chromium Insufficient validation of untrusted input in TabGroups Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8004	Chromium Insufficient policy enforcement in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8005	Chromium Insufficient validation of untrusted input in Cast Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8006	Chromium Insufficient policy enforcement in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass

CVE	NAME	PRODUCT	IMPACT
CVE-2026-8007	Chromium Insufficient validation of untrusted input in Cast Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8008	Chromium Inappropriate implementation in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-8009	Chromium Inappropriate implementation in Cast Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-8010	Chromium Insufficient validation of untrusted input in SiteIsolation Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8011	Chromium Insufficient policy enforcement in Search Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8012	Chromium Inappropriate implementation in MHTML Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-8013	Chromium Insufficient validation of untrusted input in FedCM Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8014	Chromium Inappropriate implementation in Preload Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-8015	Chromium Inappropriate implementation in Media Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-8016	Chromium Use after free in WebRTC Vulnerability	Microsoft Edge (Chromium-based)	Remote Code Execution

CVE	NAME	PRODUCT	IMPACT
CVE-2026-8017	Chromium Side-channel information leakage in Media Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-8018	Chromium Insufficient policy enforcement in DevTools Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8019	Chromium Insufficient policy enforcement in WebApp Vulnerability	Microsoft Edge (Chromium-based)	Security Feature Bypass
CVE-2026-8020	Chromium Uninitialized Use in GPU Vulnerability	Microsoft Edge (Chromium-based)	Information Disclosure
CVE-2026-8021	Chromium Script injection in UI Vulnerability	Microsoft Edge (Chromium-based)	Spoofing
CVE-2026-8022	Chromium Inappropriate implementation in MHTML Vulnerability	Microsoft Edge (Chromium-based)	Spoofing

References

https://msrc.microsoft.com/update-guide/releaseNote/2026-may

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 13, 2026 • 11:00 PM

More at www.hivepro.com